70T01019Q7NHRM074

Transportation Security Administration

Suicide Prevention Gatekeeper Training

Table of Contents

SECTION 1 - SCHEDULES OF SUPPLIES/SERVICES

1.1. General

The Transportation Security Administration (TSA) seeks to procure Suicide Prevention Gatekeeper Training in accordance with the Performance Work Statement.

1.2. Contract line item numbers

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
0001	Gatekeepers Course Available Online 24/7 for 365 days.	1	LOT		
0002	1-Day Train the Trainer Course	2	EA		
TOTAL					

SECTION 2 – PERFORMANCE WORK STATEMENT

GENERAL INFORMATION

This is a non-personal services contract to provide evidence based suicide intervention (gatekeeper) prevention training for TSA selected employees. United States Transportation Security Administration (TSA) shall not exercise any supervision or control over the contractor's service providers performing the services herein. Such service providers shall be accountable solely to the Contractor who, in turn is responsible to the government.

1. **Description of Services/Introduction:** The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform evidence based gatekeeper intervention suicide prevention training as defined in this Performance Work Statement (PWS) except for items specified as government furnished property and government services. The contractor shall perform to the standards in this contract.

   Gatekeeper intervention training refers to programs that seek to develop individuals' "...knowledge, attitudes and skills to identify (those) at risk, determine levels of risk, and make referrals when necessary" (Gould et al., 2003).

2. **Scope of Work:** Contractor will provide gatekeeper intervention suicide prevention training on two levels:

   - A self-completed gatekeeper course for TSA selected employees available online individually 24/7.
   - A one-day classroom based train the trainer course for a group(s) of TSA identified employees, between 30-50 personnel.

3. **Background:** The most recent workplace suicide of a Transportation Security Officer (TSO) plunging to his death inside Orlando International Airport shocked the Agency and together with the accompanying media coverage alerted the Agency to the growing, disturbing national public-health crisis. TSA averages between 5 and 15 documented employee suicides per year. Further Agency concerns involve undocumented employee suicides attempts that based on national averages could implicate a 500 or more employees each year. In addition to the suicidal employee's well-being, an employee considering suicide is not likely focused on their security screening responsibilities. If work or job performance issues are involved, the employee presents an increased risk of workplace violence or malevolent action using their access to public and secured areas of the airport. To improve the resiliency of the TSA workforce and reduce security risks associated with suicidal employees, the TSA Administrator has elevated suicide prevention training a priority senior leadership goal in his 2019-20 "Administrator's Intent" directive.

4. CONTRACTOR REQUIREMENTS

4.1. **Technical Requirements/Tasks:** The training product and delivery methods will:

Have been evaluated, reviewed, and certified or recommended by a recognized professional organization, (e.g. Suicide Prevention Resource Center (SPRC), Best Practices Registry (BPR), Substance Abuse and Mental Health Services Administration's (SAMHSA), and or National Registry of Evidence-Based Programs and Practices (NREPP)). All interventions will have met NREPP registry's minimum requirements for review and have been independently assessed and rated for quality of research for readiness to disseminate.

4.1.1. Require no prerequisite training

4.1.2. Offered with two levels of training:

4.1.2.1. An online course or webinar deliver self-completed gatekeeper intervention course that is

4.1.2.1.1. Available 24/7 with a help desk or customer service response process for issues related to the online training program

4.1.2.1.2. Securely accessible by individual pass code or similar access protection

4.1.2.1.3. Taught in a clear, concise format using the latest in educational technology and practices

4.1.2.1.4. Takes approximately one, but less than 3 hours to complete

4.1.2.1.5. With key components in training:

How to Question, Persuade and Refer someone who may be suicidal

How to get help for yourself or learn more about preventing suicide

The common causes of suicidal behavior

The warning signs of suicide

How to get help for someone in crisis

4.1.2.2. At least one classroom based train the trainer certification course offering:

4.1.2.2.1. Training participants to teach gatekeeper intervention training for suicide prevention including:

Understanding the nature and range of suicidal communications

Knowing the groups at greatest risk of suicide and why intervention can work for them

Suicide and suicide prevention in history

Gatekeeper training; how, why and the research

New and promising approaches to suicide prevention

How gatekeeper intervention methods fit into national efforts

4.1.2.2.2. Training delivered for 35-50 TSA identified employees

4.1.2.2.3. Result in Gatekeeper Trainer Certification

4.1.2.2.3.1. Certificate

4.1.2.2.3.2. If possible, CEU requirements

4.1.2.2.4. Rights to reproduce sets of vendor produced gatekeeper intervention suicide prevention training materials (everything needed to conduct a gatekeeper training workshop) for use by vendor certified TSA Trainers' when conducting gatekeeper training of TSA employees for a period of 12 months after the last vendor train the trainer class attending trainee.

5. **DELIVERABLES / SCHEDULE:**

Key Deliverables: Online training

Item No.	Quantity	Deliverable	Objective	Due
1	Unlimited	Online training platform available 24/7 for a period of 12 months after contract award.	Allow selected TSA employees access to online training no matter their location or time zone.	No later than five (5) business days after contract award
2	Monthly	List of personnel that attended the training session	To identify TSA personnel, location, and date of when training session was issued and provided.	Following each training sessions

Key Deliverables: Train the Trainer Course

Item No.	Quantity	Deliverable	Objective	Due
1	2	One-day classroom based train the trainer training for up to 50 TSA selected employees. One course will be held at or near TSA Headquarters in Arlington, Virginia, with a second course held near a major airport west of the Mississippi River.	Training select group of employees to provide ongoing peer intervention training, as needed, when needed, where needed to maintain available intervention coverage at all worksites.	No later than ninety (90) business days after contract award.
2	1	Limited rights for TSA to reproduce vendor produced master copy of gatekeeper training materials.	Rights to reproduce vendor provided electronic copy and master copy of gatekeeper training materials; (everything needed to conduct a gatekeeper training workshop) for use by vendor certified TSA Trainers' when conducting gatekeeper training of TSA employees for a period of 12 months after vendor completes the last vendor train the trainer class.	Master set of training materials delivered No later than ten (10) business days after the completion of the first train the trainer class.

6.0 TRAVEL: Travel costs shall be included in the firm-fixed-price of contract line item 0002. Travel in support of this effort is expected for 3 days for each class (2 travel days and 1 in-class day), at the following TSA training locations:

- At or in close proximity to TSA Headquarters in Arlington, Virginia.

- At or in close proximity to a major airport west of the Mississippi River. The government will provide the airport address not later than 2-weeks prior to the training date.

7.0 CONTRACTOR'S KEY PERSONNEL:

Account manager – main contact with authority for contract oversight and delivered service performance.

8.0 DATA RIGHTS: TSA shall have limited rights to reproduce vendor provided electronic copy and master copy of gatekeeper training materials; (everything needed to conduct a gatekeeper training workshop). This will be for use by vendor certified TSA Trainers' when conducting gatekeeper training of TSA employees for a period of 12 months after contract completion date.

9.0 INFORMATION TECHNOLOGY CLAUSES

Information Assurance Requirements for TSA Government Acquisitions (April 2016)

A. General Security Requirements

A.1. The Contractor shall comply with all Federal, Department of Homeland Security (DHS) and Transportation Security Administration (TSA) security and privacy guidelines in effect at the time of the award of the contract, as well as those requirements that may be discretely added during the contract.

A.2. The Contractor shall perform periodic reviews to ensure compliance with all information security and privacy requirements.

A.3. The Contractor shall comply with all DHS and TSA security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 standards.

A.4. The Contractor shall include this guidance in all subcontracts at any tier where the subcontractor is performing the work defined in this statement of work (SOW).

A.5. The Contractor shall ensure all staff have the required level of security clearance commensurate with the sensitivity of the information being accessed, stored, processed, transmitted or otherwise handled by the System or required to perform the work stipulated by

the contract. At a minimum, all Contractor staff shall be subjected to a Public Trust background check and be granted a Public Trust clearance before access to the System or other TSA resources is granted.

A.6. The Contractor shall sign a DHS Non-Disclosure Agreement (NDA) within (30) calendar days of the contract start date.

A.7. The Contractor shall not release, publish, or disclose agency information to unauthorized personnel, and shall protect such information in accordance with the provisions of the pertinent laws and regulations governing the confidentiality of sensitive information.

A.8. The Contractor shall ensure that its staff follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel shall be responsible for the physical security of their area and government furnished equipment (GFE) issued to the contractor under the terms of the contract.

A.9. The Contractor shall make all system information and documentation produced in support of the contract available to TSA upon request.

B. Training Requirements

All Contractor employees, requiring system access, shall receive initial Organizational Security Fundamentals Training within 60 days of assignment to the contract via the Online Learning Center (OLC). Refresher training shall be completed annually thereafter.

B.1. The Contractor shall complete annual online training for Organizational Security Fundamentals and TSA Privacy training.

B.2. Role Based training is required for contract employees with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, and shall be in accordance with DHS and TSA policy. The contractor will be notified if they have a position with significant security responsibility.

B.3. Individuals with SSR shall have a documented individual training and education plan, which shall ensure currency with position skills requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan shall be refreshed annually or immediately after a change in the individual's position description requirements.

B.4. Information Security and Privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

B.5. The Contractor shall maintain a list of all employees who have completed training and shall submit this list to the contracting officer representative (COR) upon request, or during DHS/TSA onsite validation visits performed on a periodic basis.

B.6. The contractor shall its employees review and sign the TSA Form 1403 Computer and Wireless Mobile Device Access Agreement (CAA) prior to accessing IT systems.

C. Configuration Management (hardware/software)

C.1. Hardware or software configuration changes shall be in accordance with the DHS Information Security Performance Plan (current year and any updates thereafter), the DHS Continuous Diagnostics and Mitigation (CDM) Program to include dashboard reporting requirements and TSA's Configuration Management policy. The TSA Chief Information Security Officer (CISO)/Information Assurance and Cyber Security Division (IAD) shall be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD POC shall approve any request for change prior to any development activity occurring for that change and shall define the security requirements for the requested change. The COR will provide access to the DHS Information Security Performance Plan.

C.2. The Contractor shall ensure all application or configuration patches and/or Requests for Change (RFC) have approval by the Technical Discussion Forum (TDF), Systems Configuration Control Board (SCCB) and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 Information Technology Security and TSA Information Assurance (IA) Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA CISO, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

C.3. The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.

C.4. The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting "sensitive information") shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/NIST, National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

C.5. US Government Configuration Baseline and DHS Configuration Guidance

a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB) and in accordance with DHS and TSA guidance.

1. USGCB Guidelines:
    a. http://usgcb.nist.gov/usgcb_content.html
2. DHS Sensitive Systems Configuration Guidance

a. http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx

b) The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology shall also use the Windows Installer Service for installation to the default "program files" directory and shall be able to discretely install and uninstall.

c) Applications designed for general end users shall run in the general user context without elevated system administration privileges.

C.6. The Contractor shall establish processes and procedures for continuous monitoring of Contractor systems that contain TSA data/information by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). The Contractor shall perform monthly security scans on servers that contain TSA data, and shall send monthly scan results to the TSA IAD.

D. Risk Management Framework

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

D.1. The Security Authorization and Ongoing Authorization Process in accordance with NIST SP 800-37 and SP 800-137 (current versions) is a requirement for all TSA IT systems, including General Support Systems (e.g., standard TSA desktop, general network infrastructure, electronic mail), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework (RMF). Ongoing Authorization is part of Step 6 "Monitoring" of the RMF. All NIST guidance is publicly available; TSA and DHS security policy is disclosed upon contract award with some exceptions, which are public facing (i.e., DHS Security and Training Requirements for Contractors).

D.2. A written Authorization to Operate (ATO) granted by the TSA Authorizing Official (AO) also known as TSA Chief Information Security Officer (CISO) is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.

D.3. TSA shall assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) Pub 199 *Standards for Security Categorization of Federal Information and Information Systems* impact levels and assign security controls to those systems consistent with FIPS Pub 200 *Minimum Security Requirements for Federal Information and Information Systems* methodology.

D.4. Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation shall be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

D.5. The Security Authorization (SA)Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation: 1) Security Assessment Report (SAR), 2) Security Plan (SP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Security Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Assessment Plan (SAP), 9) Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Ongoing Authorization Artifacts as required by the DHS Ongoing Authorization Methodology (current version). The SA package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents shall be reviewed and approved by the CISO and the IAD, and accepted by the CO upon creation and after any subsequent changes, before they go into effect. Ongoing Authorization artifacts include monthly TRigger Accountability Log (TRAL), monthly operating system scan results, application scans as directed, updated control allocation table (CAT), and associated memos as directed. All steps in the DHS Information Assurance Compliance Systems (IACS) shall be completed correctly, thoroughly and in a timely manner for all steps of the RMF.

D.6. The contractor shall support the successful remediation of all identified system weaknesses and vulnerabilities that are identified as a result of the aforementioned security review process.

D.7. The contractor shall submit and analyze monthly operating system vulnerability scans for the DHS Information Security Performance Plan FISMA Scorecard. Vulnerabilities not remediated are generated into Plan of Action and Milestone (POA&M)s after 30 days.

E. Contingency Planning

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

E.1. The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations may be disrupted and thus require activation of the CP and/or COOP. are disrupted. The contractor's CP/COOP responsibility relates only to the system they provide or operate under contract.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in the DHS IACS Tool. If access has not been provided initially, the contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K *IT Contingency Plan Template*.

E.3. The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

E.4. The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

E.5. The Contractor shall test their CP annually and retain records of the annual CP testing for review during periodic audits.

E.6. The Contractor shall record, track, and correct any CP deficiency; any deficiency correction that cannot be accomplished within one month of the annual test shall be elevated to IAD.

E.7. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.8. The Contractor shall have an Emergency Response Plan that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other incident or activity that may endanger lives, property, or the capability to perform essential functions.

E.9. The Contractor shall have a Backup Operations Plan that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason.

E.10. The Contractor shall have a Post-disaster Recovery Plan that includes procedures and responsibilities to facilitate rapid restoration of normal operations at the primary site or, if necessary, at a new facility following the destruction, major damage, or other major interruption at the primary site.

E.11. The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

E.12. The Contractor shall ensure a full backup of all network data occurs as required by the system's availability security categorization impact rating per TSA Information Assurance policy.

E.13. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) shall be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one hour.

E.14. The Contractor shall ensure sufficient backup data to facilitate a full operational recovery within one business day at either the prime operational site or the designated alternate site shall be stored at a secondary location determined by the local element disaster recovery plan.

E.15. The Contractor shall ensure that data at the secondary location is current as required by the system's availability security categorization impact rating.

E.16. The Contractor shall ensure the location of the local backup repository and the secondary backup repository is clearly defined, and access controlled as an Information Security Restricted Area (ISRA).

E.17. The Contractor shall adhere to the DHS IT Security Architecture Guidance Volume 1: *Network and System Infrastructure* for the layout of the file systems, or partitions, on a system's hard disk impacting the security of the data on the resultant system. File system design shall:

- Separate generalized data from operating system (OS) files
- Compartmentalize differing data types
- Restrict dynamic, growing log files or audit trails from crowding other data

E.18. The contractor shall adhere to the DHS IT Security Architecture Guidance Volume 1: *Network and System Infrastructure* for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

F. Program Performance

F.1. The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the Contracting Officer (CO).

F.2. The Contractor shall provide support during the IAD audit activities and efforts. These audit activities shall include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

F.3. Upon completion of monthly security scans, findings shall be documented and categorized as High, Moderate, or Low based on their potential impact to the System IT Security posture. The Contractor shall provide TSA with estimates of the total engineering service hours required to support the remediation of open POA&M items. High security findings shall be remediated first in 45 days or less; Moderate security findings shall be remediated in 60 days or less, and Low security findings shall be remediated in 90 days or less. The Contractor shall work with the TSA System ISSO and the respective CO and/or Contracting Officer's Representative (COR), as well as OIT IAD and the System Owner (as required) to prioritize and plan for the remediation of open POA&Ms. The TSA System ISSO shall maintain all security artifacts and perform Ongoing Authorization (per NIST 800-137 and DHS-TSA requirements) and Continuous Diagnostics and Mitigation (CDM) (per OMB M-14-03) activities to ensure active compliance with security requirements. Specific POA&M guidance and information can be found in the SOP 1401 *Plan of Action and Milestone (POA&M) Process*, as well as the DHS 4300A PD Attachment H *Plan of Action and Milestones (POA&M) Process Guide.*

G. Federal Risk and Authorization Management Program (FedRAMP)

If a vendor is to host a system with a Cloud Service Provider, the following shall apply:

G.1. **FedRAMP Requirements**: Private sector solutions shall be hosted by a Joint Authorization Board (JAB)-approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) (http://cloud.cio.gov/fedramp/cloud-systems) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The CSP shall adhere to the following in addition to the FedRAMP requirements:

- Identity and entitlement access management shall be done through Federated Identity;
- SSI and PII shall be encrypted in storage and in transit as it is dispersed across the cloud;
- Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS or SaaS levels;
- Cloud bursting shall not occur;
- TSA data shall be logically separated from other cloud tenants;
- All system administrators shall be properly cleared and vetted U.S. citizens;
- TSA data shall not leave the United States; and
- The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has EINSTEIN 3 Accelerated (E3A) capabilities deployed. These include but are not limited to the analysis of network flow records, detecting and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The E3A capability shall use the Domain Name Server Sinkholing capability and email filtering capability allowing scans to occur destined for .gov networks for malicious attachments, Uniform Resource Locators and other forms of malware before being delivered to .gov end-users.

G.2. Private Sector System Requirements: TSA shall conduct audits at any time on private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS IACS. The private sector systems are required to go through the Security Authorization Process and the RMF in accordance the Federal Information Systems Management Act (FISMA) and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has E3A deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Management Directive 1400.3 and its Attachment 1 (TSA IA Handbook) shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS and communicated by the contracting officer representative (COR) or contract security point of contact (POC).

H. Information Assurance Policy

H.1. All services, hardware and/or software provided under this task order shall be compliant with applicable DHS 4300A Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook, TSA MD 1400.3 Information Technology Security, TSA IA Handbook, Technical

Standards (TSs) and standard operating procedures (SOPs).

H.2. The contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which shall be provided by the Contracting Officer.

H.3. Authorized access and use of TSA IT systems and resources shall be in accordance with the TSA IA Handbook.

H.4. The contractor shall complete TSA Form 251 and TSA Form 251-1 for sensitive or accountable property. The contractor shall email the completed forms to TSA-Property@dhs.gov and include a hard copy with the shipment.

I. Data Stored/Processed at Contractor Site

I.1. Unless otherwise directed by TSA, any storage of data shall be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

J. Remote Access Contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct sanctioned TSA business. Therefore, remote access rights shall be expressly granted, in writing, by the TSA IAD.

J.1. The Contractor employee(s) remote access connection to TSA networks shall be terminated immediately for unauthorized use, at the sole discretion of TSA.

J.2. The Contractor shall use his or her federal issued personal identifiable verification (PIV) badge to access TSA resources to include IT applications and physical facility.

K. Interconnection Security Agreement

If the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity, the following shall apply:

K.1. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented using an interagency agreements; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

K.2. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

K.3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

L. SBU Data Privacy and Protection

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

L.1. The contractor shall satisfy requirements to work with and safeguard Sensitive Security Information (SSI), Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (Sensitive PII). All support personnel shall understand and rigorously follow DHS and TSA requirements, SSI Policies and Procedures Handbook, and Privacy policies, and procedures for safeguarding SSI, PII and SPII.

L.2. The Contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor's control. All TSA data, including but not limited to PII, SPII, Sensitive Security Information (SSI), Sensitive But Unclassified (SBU), and Critical Infrastructure Information (CII), shall be protected according to DHS and TSA security policies and mandates.

L.3. TSA shall identify IT systems transmitting unclassified/SSI information that shall require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2 (current version)

National Security Agency (NSA) Type 2 or Type 1 encryption (current version)

Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the DHS 4300A Sensitive Systems Handbook), current version

L.4. The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII shall comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

L.5. Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA IA Handbook, and applicable IT Security Technical Standards and SOPs.

L.6. The contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA IA Handbook, applicable Technical Standards, SOPs and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

L.7. The Contractor shall ensure that source code is protected from unauthorized access or

dissemination (see TSA IA Handbook).

M. Disposition of Government Resources

M.1 At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA IA Handbook, Technical Standards and SOPs. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, TSA Technical Standard 046 *IT Media Sanitization and Disposition*, and SOP 1400-503 *IT Media Sanitization*. The contractor shall email a signed, by the contractor's designated security officer or senior official, proof of sanitization to the COR. In addition, the contractor shall provide the contracting officer a master asset inventory list that reflects all assets, government furnished equipment (GFE) or authorized non-GFE that were used to process TSA information.

N. Special Considerations and Circumstances (if applicable and when requested)

N.1 For major agency Information Technology (IT) infrastructure support ranging in the total estimated procurement value (TEPV) of about $100 million or above **or** per TSA management's request, the contractor shall provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA IAD. This plan shall describe the processes and procedures that shall be followed to ensure the appropriate security of IT resources are developed, processed, or used under this contract. At a minimum, the contractor's SPP shall address the contractor's compliance with the controls described in NIST SP 800-53 (current version). The security controls contained in the plan shall meet the requirements listed in the TSA IA Handbook, Technical Standards and the DHS Sensitive Systems Policy Directive and Handbook 4300A (current versions).

N.2 The SPP shall be a living document. It shall be reviewed and updated semi-annually, beginning on the effective date of the contract, to address new processes, procedures, technical or federally mandated security controls and other contract requirement modifications or additions that affect the security of IT resources under contract.

N.3 The SPP shall be submitted within 30 days after contract award. The SPP shall be consistent with and further details the approach contained in the Offerors proposal or quote that resulted in the award of this contract and in compliance with the system security requirements.

N.4 The SPP, as submitted to the Contracting Officer, and accepted by the Information Systems Security Officer (ISSO), shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

O. Trusted Internet Connection 2.0 Requirements for Managed Trusted Internet Protocol Service Offering (MTIPS)

O.1 MTIPS providers shall comply with the FedRAMP TIC 2.0 Overlay requirements in addition to the basic requirements outlined in the DHS TIC Reference Architecture v2.0.

P. ISSO Support

P.1 The contractor Program Manager shall ensure that the contractor ISSO duties and responsibilities align with the Information Assurance and Cyber Security Division, Governance, Risk, and Compliance (GRC) Branch mission and security responsibilities. The TSA CISO is the authorizing official for ISSO designation.

Q. Continuous Diagnostics and Mitigation

Q.1 The Government, through a Continuous Monitoring as a Service (CMaaS) vendor, shall provide the contractor with GFE appliances and tools to support the implementation and maintenance of the Continuous Diagnostics and Mitigation (CDM) Solution. The tools shall be hosted on the DHS' Infrastructure as a Service (IaaS) program. The Government, through the CMaaS vendor, shall provide sensor kits and agents that shall be deployed on all contractor Information Systems supporting the TSA.

Q.2 The contractor shall support the installation (including rack and configuration) of the sensor kits and agents on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards.

Q.3 The contractor shall tune their existing endpoint security products to coexist with the identified products to ensure smooth and cohesive functionalities. Credentials (Service accounts) shall be provided, by the TSA CISO or designee, for vulnerability scans and host interrogation.

Q.4 The Government, through the CMaaS vendor, shall provide the following support for operations and maintenance of the CDM solution sensor kits:

- Patching (Controlled through a CMaaS Windows Server Update Service (WSUS))
- Hardware troubleshooting & Risk Management (RMA)
- Application maintenance (done from the Government/TSA Management Enclave)
- Vulnerability scanning

Q.5 The contractor shall install TSA-provided CDM Solution patches within two (2) days of issuance, or as directed by TSA, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

Q.6 The TSA Contracting Owner is authorized to provide technical direction to the contractor for the sole purpose of implementing the CDM Solution. If the technical direction results in any cost incurred by the contractor, for which the contractor shall seek reimbursement from the Government, the contractor shall identify the following information in any cost/price proposal to the Government: name of system owner, summary of the technical direction, date of the technical direction, purpose of the technical direction, summary of actions taken by the contractor, any other information the contracting officer may require to further guide the directed change. The contactor shall receive approval from the Contracting Officer of the directed change prior to incurring costs associated with the technical direction.

R. Software Guidance

The Contracting Officer shall provide a listing of all TSA approved security software upon contract award. The approved security software listing is maintained by the Information Assurance Division (IAD).

R.1 In support of the CDM objective to protect high value assets (HVAs) and information, the Government has acquired security tools in order to conduct Indicator of Compromise (IOC) scans within the mandated time frame. The Government shall provide the tool license and/or equipment for installation of tool agents on all TSA supported assets.

R.2 The contractor shall support efforts to allow for the IOC scanning mandate. This may include installation of tool servers and/or agents within each system's environment and on all TSA supported assets. The Government shall provide the contractor with the tool server(s) that shall not belong to the contractor's system boundary. The tool server shall be reachable from OneNet/TSANet over the Internet. The tool server(s) shall be properly configured to reach all assets with the tool agent installed on the network. Credentials (service accounts) shall be provided for IOC scans and tool interrogation.

R.3 The contractor shall support or perform the installation of forensic software servlet agents on supported Operating Systems on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards. The contractor shall test and upgrade the servlet agents as directed by the IAD.

R.4 The Government shall provide the contractor with a forensic software server that shall not belong to the contractor's system boundary. The contractor shall support or perform the installation of the server. The server shall be reachable from TSANet over the Internet and shall be primarily used for authentication and proxy functions. The server shall be properly configured to reach all assets with the agent installed on the network.

R.5 The contractor shall support efforts of incident response and forensic investigation. This includes authorization to connect TSA authorized equipment where the forensic software servlet agents are reachable to perform analysis.

R.6 The contractor shall install TSA-provided solution patches within two (2) days of

issuance, or as directed by TSA CIO, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

S. Passwords

S.1 The contract ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation. In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.

T. Personal Identifiable Verification (PIV)

T.1 The Contractor shall use PIV as the primary means to access TSA resources to include IT applications and physical facility. TSA network domain user account password expiration function shall be disabled when using PIV Machine Based Enforcement (MBE). PINs for PIV card-enabled users shall not expire, and shall have a minimum six-digit PIN when logging into the network using a PIV card.

T.2 The Contractor shall ensure newly developed information system(s) support PIV smartcard authentication. The information system shall be capable to accept and electronically verify PIV credentials.

T.3 The Contractor shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. http://www.idmanagement.gov/approved-products-list.

T.4 The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to TSA's facilities, networks, and information systems.

U. End-of-Life (EOL) / End-of-Service (EOS)

U.1 The Contractor shall ensure that any hardware or software that is procured develops a full lifecycle plan based on the vendor's established life and service expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within three (3) years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the TSA CISO in order to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

V. Maintenance

V.1 The Contractor shall ensure that the system, once operational, is properly maintained and monitored, to include: immediate response to critical security patches, routine maintenance windows to allow for system updates, and compliance with a defined configuration management process. All patches and system updates shall be properly tested in a development environment before being implemented in the production environment.

V.2 The contractor shall perform customer support twenty-four (24) hours, seven (7) days a week within the continental United States only.

W. Security in the Agile Development Process

All TSA systems shall follow the below guidance when delivering system and application solutions to the agency.

- All applications shall be reviewed prior to acceptance by the Contractor
- Contractor shall implement Threat Modeling
- Developer shall deliver a defect list
- Developer shall implement Patching and Configuration Management strategies
- Developer shall use Component Analysis
- Developer shall implement build tests
- Developer shall implement Manual Code Inspection
- Developer shall implement Security Regression Tests
- Developer shall implement Pre-Deployment/Post Deployment Automated Tests
- Developer shall implement industry standard "Every-Sprint Practices", which at a minimum consists of:
    - Threat Modeling
    - Use of Approved Tools
    - Deprecate Unsafe Functions
    - Static Analysis
    - Conduction Final Security Review
    - Certify, Release and Archive

- Developer shall implement industry standard Practices, which at a minimum consists of:
    - Create Quality Gates/Bug Bars
    - Perform Dynamic Analysis
    - Perform Fuzz Testing
    - Conduct Attach Surface Review

- Developer shall implement industry standard One-Time Practices, which at a minimum

consists of:

- Establish Security Requirements
- Perform Security and Privacy Risk Assessments
- Establish Design Requirements
- Perform Attack Surface Analysis
- Create Incident Response Plan

DHS and TSA Enterprise Architecture Compliance

a) The Contractor shall ensure that all solutions, products, deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the Federal Enterprise Architecture Framework (OMB Reference Models).

b) All solutions and services shall meet DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with Homeland Security Enterprise Architecture (HLS EA) requirements.

i. All developed solutions and requirements shall be compliant with the HLS EA.

ii. The contractor shall align all solutions and services and ensure compliance with applicable TSA and DHS IT Security, Application, System, Network, Data, Information, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.

iii. The contractor shall utilize any existing TSA or DHS user interface design standards, style guides, and/or policies and standards for human factors, usability, user experience, or human computer interaction (HCI).

iv. All solution architectures and services (Application, System, Network, Security, Information, etc.) shall be reviewed and approved by TSA EA as part of the TSA SELC review process and in accordance with all applicable DHS and TSA IT governance policies, directives, and processes (i.e. TSA IT Governance Management Directive 1400.20). This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. All implementations shall follow the approved solution architecture/design without deviation. Any changes, to either the prior approved solution and/or prior approved design that are identified during subsequent SELC phases, including testing, implementation and deployment, shall undergo additional EA review prior to proceeding.

v. All IT hardware and software shall be compliant with the TSA and HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products

are subject to TSA and DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the TSA and HLS EA TRM Standards and Products Profile.

c) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the TSA Enterprise Architecture Data Management Team, who will be responsible for coordination with the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

i. Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS and TSA data management architectural guidelines and subject to the TSA Enterprise Architecture Data Management Team (EDM) approval.

ii. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – 'Rights in Data and Copyrights' and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in an understandable format to TSA. Examples of data structures can be defined as, but not limited to

a. Data models depicting relationship mapping and, or linkages
b. Metadata information to define data definitions
c. Detailed data formats, type, and size
d. Delineations of the referential integrity (e.g., primary key/foreign key) of data schemas, structures, and or taxonomies

iii. All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within the 'Requirements for Handling Sensitive, Classified, and/or Proprietary Information', section of this SOW. This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system. Alternative data delivery techniques may also be defined by TSA Enterprise Data Management (EDM) team.

iv. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g. metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered

in a TSA approved manner). Metadata shall also provide an indication of historical verses the most current data to be used, as well as frequency of data refreshes.

v. The contractor shall adhere to providing a Data Management Plan (DMP), as defined by Enterprise Architecture, to the EA design review team before the preliminary/critical design review. The Data Management Plan includes conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data. All data artifacts must adhere to TSA EA data standards defined and published before the design review. Data Standards include but are not limited to, data asset standards, metadata standards, logical/physical naming standards, and information exchange (using the National Information Exchange Model (NIEM)) standards. All required artifacts must be provided to and approved by the EA Design Review team.

d) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

SECURITY REQUIREMENTS FOR HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE (JULY 2017)

1. Definitions.

(a) "Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

(b) "Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource

locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

2. Systems Security.

(a) Use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:

(i) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(ii) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;

(iii) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;

(iv) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.

(v) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;

(vi) Contractor employee training requirements are covered in FAR 52.224-3.

(vii) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

3.Data Security.

(a) Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract.

(b) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain Sensitive PII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

4. Breach Response. The contractor agrees that in the event of any actual or suspected breach of SPII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer, the Contracting Officer's Representative (COR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov<mailto:TSAprivacy@tsa.dhs.gov>). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. The report of a breach shall not, by itself, be interpreted as evidence that the contractor failed to provide adequate safeguards for SPII.

Award fee contracts:

(a) For any portions of this contract that involve an award fee, the contractor may be awarded no award fee for any evaluation period in which there is a breach of privacy or security, including any loss of sensitive data or equipment containing sensitive data. Lost award fee due to a breach of privacy or security may not be allocated to future evaluation periods.

(b) For any portions of this contract that involve an award fee, to ensure that the final award fee evaluation at contract completion reflects any breach of privacy or security in an interim period, the overall award fee pool shall be reduced by the amount of the fee available for the period in which the breach occurred if a zero fee determination was made because of a breach of privacy or security.

5. Personally Identifiable Information Notification Requirement.

(b) In the event that a PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not less than18 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts

under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): suicide intervention training

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Electronic documents; Electronic forms; Electronic reports; Electronic training materials): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply, except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, and 3.2.4 Consistent Identification

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms): All requirements in

Chapter 5 apply, including all WCAG Level AA Success Criteria Apply except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, 3.2.4 Consistent Identification, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance-test-processes.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.0 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be

explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each ICT Item that will be developed, modified, installed, configured, integrated, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

3. The offeror shall describe plans for features that do not fully conform to the Section 508 Standards.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

    - Accessibility test results based on the required test methods.
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

SECTION 3 – TSA SPECIAL CONTRACT REQUIREMENTS

G. 5200.243.001 CONTRACTING OFFICER (CO) (JUL 2015)

The Contracting Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue orders, obligate funds and authorize the expenditure of funds, and notwithstanding any term contained elsewhere in this contract, such authority remains vested solely in the Contracting Officer. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) In the event, the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:

NAME: Ms. Sophia Woodward
PHONE NUMBER: 571-227-4580
EMAIL: sophia.woodward@tsa.dhs.gov

(End of term)

G.5200.242.001 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AND TECHNICAL MONITORS (JUL 2015)

The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

TSA CORs:

NAME:	Mr. Leon Patton
PHONE NUMBER:	571-227-4688
EMAIL:	Leon.Patton@tsa.dhs.gov

The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

The responsibilities and limitations of the COR are as follows:

- The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
- The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
- The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
- The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
- The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
- The COR is not authorized to direct the Contractor on how to perform the work.
- The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
- The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

The responsibilities and limitations of the TM are as follows:

- Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

- Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
- Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
- Informing the COR if the Contractor is not meeting performance, cost, schedule milestones.
- Performing technical reviews of the Contractor's proposals as directed by the COR.
- Performing acceptance of the Contractor's deliverables as directed by the COR.
- Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

(End of term)

G.5200.242.003 SUBMISSION OF INVOICES (JUL 2015)

Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

A. **Invoice Submission Method**: Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:

1. Facsimile number is: 757-413-7314

The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (d) of this term.

2. Address to mail invoices:
United States Coast Guard Finance Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake, VA 23327-4111

3. Email Address: FIN-SMB-TSAInvoices@uscg.mil or www.fincen.uscg.mil

B. **Invoice Process**: Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

C. **Discounts on invoices**. If desired, the Contractor should offer discounts directly upon the invoice submitted, clearly specifying the terms of the discount. Contractors can structure discounted amounts for payment for any time period less than the usual thirty day payment period specified under Prompt Payment requirements; however, the Contractor should not structure terms for payment of net amounts invoiced any sooner than the standard period required under FAR Subpart 32.9 regarding prompt payments for the specified deliverables under contract.

Discounts offered after invoice submission. If the Contractor should wish to offer a discount on a specific invoice after its submission for payment, the Contractor should submit a letter to the Finance Center identifying the specific invoice for which a discount is offered and specify the exact terms of the discount offered and what time period the Government should make payment by in order to receive the discount. The Contractor should clearly indicate the contract number, invoice number and date, and the specific terms of the discount offered. Contractors should not structure terms for net amount payments any sooner than the standard period required under FAR Subpart 32.9 regarding prompt payments for the specified deliverables under contract.

D. **Payment Status**: Contractors may inquire on the payment status of an invoice by any of the following means:

1. Via the internet: https://www.fincen.uscg.mil

Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

2. Via the Payment Inquiry Form: https://www.fincen.uscg.mil/secure/payment.htm

E. **Invoice Elements**: Invoices will automatically be rejected if the information required in subparagraph (a)(2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and DUNS number are not included in the invoice. All invoices must clearly correlate invoiced amounts to the corresponding contract line item number and funding citation. The Contractor shall work with the Government to mutually refine the format, content and method of delivery for all invoice submissions during the performance of the Contract.

F. **Supplemental Invoice Documentation**: Contractors shall submit all supplemental invoice documentation (e.g. copies of subcontractor invoices, travel vouchers, etc.) necessary to approve an invoice along with the original invoice. The Contractor invoice must contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Representative. Note for "time-and-material" type contracts: The Contractor must submit the following statement with each invoice for labor hours invoiced under a "time-and-materials" type contract, order, or contract line item: "The Contractor hereby certifies in accordance with paragraph (c) of FAR 52.232-7, that each labor hour has been performed by an employee (prime or subcontractor) who meets the contract's specified requirements for the labor category invoiced."

G. **Additional Invoice Preparation Instructions for Software Development and/or Hardware**. The Contractor shall clearly include a separate breakdown (by CLIN) for any software development activities (labor costs, subcontractor costs, etc.) in accordance with Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10 (Preliminary design costs, Development costs and post implementation costs) and cite payment terms. The contractor shall provide make and model descriptions as well as serial numbers for purchases of hardware and software (where applicable.)

H. **Frequency of Invoice Submission**. Invoices shall be submitted on a monthly basis in accordance with the schedule.

(End of term)

H.5200.204.002 CONTRACTOR PERSONNEL ACCESS TO TSA FACILITIES, INFORMATION AND/OR SYSTEMS (SEP 2018)

Prescription: The Contracting Officer shall include in all TSA contracts that require contractor employee access to TSA facilities, information systems, and/or sensitive but unclassified information. This includes contracts involving work on TSA equipment at airport checkpoints. For contracts involving performance at airports (other than work on TSA equipment at the checkpoint), this term shall be included in contracts requiring unescorted access to TSA occupied spaces.

A. All Contractor personnel requiring access to TSA facilities, information systems, and/or information will be subject to the security procedures set forth in this contract.

B. All contractor employees seeking to provide services to TSA under a TSA contract are subject to a fitness determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Law Enforcement/Federal Air Marshall Service's, Personnel Security

Section (PerSec), will allow a contractor employee to commence work on a TSA contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

C. A fitness determination involves the following three phases:
   1. Phase 1: Enter On Duty Fitness Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination may include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final fitness determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.
      When a contractor employee is deemed eligible to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Representative (COR) of the favorable determination. Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

   2. Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for final fitness adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

   3. Phase 3: Final Fitness Adjudication: TSA PerSec will complete the final fitness determination after receipt, review, and adjudication of the completed OPM background investigation. The final fitness determination is an assessment made by TSA PerSec to determine whether there is reasonable expectation that the continued employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final fitness determination will result in a notification to the COR that the contractor employee has been deemed unfit for continued contract employment and that he/she shall be removed from the TSA contract.

D. The period of performance may begin 60 days after contract award to allow for the Enter On Duty Fitness Determination. A contract modification shall be executed to revise the period of performance once the determination process is completed. For Fixed price awards, in the

event of staggered completed determinations the parties may negotiate fixed monthly rates so that performance can begin with partial staff.

E. Whenever personal identity verification (PIV) cards are required for issuance or re-issuance to contractor personnel for authorized access to Government facilities, under the guidance of the Contracting Officer's Representative (COR), the Contractor is responsible for making all arrangements for affected Contractor personnel to report in-person at the nearest Government issuing facility to initiate and complete procedures for PIV card issuance. The Government will not be able to provide PIV card issuance at any other locations than those officially designated as available. PIV card issuing facilities that are available for the completion of this requirement for TSA contractors are as listed by the TSA Personnel Security Section, and the COR will advise the Contractor about Government PIV card issuing facility locations that are nearby the contractor's location(s) of performance that will be potentially available for card issuance when required.

H.5200.204.005 NON-FEDERAL ACCESS TO TSA NATIONAL CAPITAL REGION FACILITIES (SEP 2016)

A. Background. Department of Homeland Security (DHS) Visitor Access Policy mandates that visitors, to include all parties such as proposed subcontractors, accessing DHS National Capital Region (NCR) Component Headquarters and related Headquarters NCR facilities be subject to a criminal history check. To that end, in July 2016, TSA began requiring the submission of Personally Identifiable Information (PII) for all non-federal visitors and foreign national visitors entering TSA facilities in the National Capital Region, including TSA Headquarters, the Freedom Center, Annapolis Junction, Walker Lane, and the Transportation Security Integration Facility (TSIF), in order to process the required screening checks. Of note, for contracts requiring access to TSA facilities, information systems, or sensitive but unclassified information as part of contract performance, contractor employees are subject to a suitability determination. (See H.5200.204.002, CONTRACTOR PERSONNEL ACCESS TO TSA FACILITIES, INFORMATION AND/OR SYSTEMS).

B. Purpose: The submitted information will be used to conduct screening checks to permit and maintain records of access to DHS NCR facilities pursuant to the authority of 40 U.S.C. § 1315; 41 C.F.R. Part 102-81; Executive Order. 9397.

C. Applicability: A Non-Federal Visitor or Foreign National Visitor is an individual who has not been issued a DHS Personal Identity Verification (PIV) card or is not a current Federal government employee. Non-TSA current Federal government employees will be recorded in the Visitor Request Form excluding any PII.

D. Routine Uses: The information requested may be shared externally as a "routine use" to the Department of Justice, Federal Bureau of Investigation and other government agencies as part of the screening process. A complete list of the routine uses can be found in the system

of records notice, "Department of Homeland Security/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records."

E. Consequences of Failure to Provide Information: Providing this information, including Social Security Number (SSN), is voluntary. However, failure to provide the information requested may result in being denied access to a DHS facility; failure to provide the SSN may prevent completion of screening.

F. Information Requirements. In accordance with the above:

1. Non-Federal Visitors. Non-Federal visitors to TSA facilities will need to provide Date of Birth and Social Security Number information. The required information shall be provided in a password protected Microsoft Excel spreadsheet emailed to the Contracting Officer at least one (1) full business day prior to the visit date. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) The Contracting Officer may delegate the receipt of this information to the respective Contracting Officer Representative (COR). In order to ensure protection of this information, the password for the password protected spreadsheet shall be sent to the Contracting Officer (or delegated COR) in a separate email, at the same time. If multiple non-federal visitors from one company require access to TSA Headquarters facilities, that company should submit a single complete spreadsheet. A DHS/TSA employee shall be responsible for both inputting the information into the Visitor Request Form and actual escorting the visitor(s) at all times. The submitted emails shall then be deleted by TSA.

2. Foreign National Visitors. Foreign Nationals visiting TSA facilities in the U.S. and its territories will need to submit additional information to screening purposes, specifically:

- Date of Birth
- Gender
- Country of Citizenship
- Country of Birth
- Passport Number and Expiration Date
- Position/Title

The required information shall be provided in a password protected Microsoft Excel spreadsheet emailed to the Contracting Officer at least seven (7) full business days prior to the visit date. The Contracting Officer may delegate the receipt of this information to the respective Contracting Officer Representative (COR). In order to ensure protection of this information, the password for the password protected spreadsheet shall be sent to the Contracting Officer (or delegated COR) in a separate email, at the same time. If multiple Foreign National visitors from one company require access to TSA Headquarters facilities,

that company should submit a single complete spreadsheet. A DHS/TSA employee shall be responsible for both inputting the information into the Visitor Request Form and actual escorting the visitor(s) at all times. The submitted emails shall then be deleted by TSA.

(*End of term)*

H.5200.204.007 TSA HEADQUARTERS LOCATION CONSOLIDATION (JUL 2018)

The new Transportation Security Administration (TSA) headquarters location will be near the Franconia-Springfield Metro Station at 6595 Springfield Center Drive in Springfield, Virginia. TSA will be consolidating and physically moving its headquarters locations over a staggered period within calendar years 2020 and 2021, as currently planned. The consolidation will include existing TSA locations at:

- 6354 Walker Lane, Springfield, VA
- 1900 Oracle Way, Reston, VA
- 601/701 South 12th St., Arlington, VA

Moving expenses for contractors and/or contractor employees now assigned by their employers to perform under contract at any of these present TSA locations will not be considered or paid under contract, and plans for company employees' and their company equipment or property to these new locations will be the responsibility of the company.

Additional instructions under existing contracts for facility access instructions for contractors, visitors, and mail/parcel and other deliveries will be added to each affected contract as necessary.

(End of Term)

H.5200.205.001 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION (OCTOBER 2017)

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the award and/or performance of this contract without the prior written consent of the Contracting Officer. The Contractor shall submit any request for public release at least ten (10) business days in advance of the planned release. Under no circumstances shall the Contractor release any requested submittal prior to TSA approval.

Any material proposed to be published or distributed shall be submitted via email to the Contracting Officer. The Contracting Officer will follow the procedures in Management Directives 1700.3 and 1700.4. The Administrator retains the authority to deny publication

authorization. Any conditions on the approval for release will be clearly described. Notice of disapproval will be accompanied by an explanation of the basis or bases for disapproval.

(End of term)

H 5200.237.004 CONTRACTOR RESPONSIBILITY, CONDUCT AND PERFORMANCE UNDER TSA SERVICE CONTRACTS (JUNE 2019)

A. **BASIC REQUIRED STANDARDS OF CONDUCT RELATED TO BUSINESS UNDER GOVERNMENT CONTRACTS**

1. General. The Government has the basic inherent expectations of timely, focused, effective, and competent performance by the Contractor under a contract. The Contractor has the basic inherent expectation of fair treatment under the contract, where the Contractor's employees, when in Government facilities or in circumstances where the Government has primary control or responsibility, have the expectation of performance in a safe and non-hostile work environment.

2. Adherence to Standards. The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. See TSA Management Directive (MD) 1100.73-5, Employee Responsibilities and Code of Conduct. Contractor employees performing work under this contract shall not:
-Solicit new business (on-site at government spaces, or while on work during periods paid by Government) while performing work under the contract;
-Conduct business other than that which is covered by this contract during periods paid by the Government;
-Conduct business not directly related to this contract while on Government premises;
-Use Government computer systems or networks, Government property or materials, and/or Government facilities for company or personal business;
-Recruit while on Government premises or otherwise act to disrupt official Government business while on Government premises.
-Discuss with unauthorized persons any information obtained during the performance of work under this contract.-
-Engage in harassment . See TSA MD 1100-73.3 Anti-Harassment Program .

3. Reporting Matters.
Illegal, and Unethical, or Inappropriate Conduct. The Contractor, and its employees shall immediately report to the Contracting Officer and/or Contracting Officer's Representative, any illegal, or unethical, or inappropriate conduct observed, noticed, or discovered while on Government premises or during periods paid by the Government under this contract, without regard as to the source of such conduct (except that any matter involving only contractor employees, apart from any Government requirements or the specific requirements of this contract, is deemed to be strictly the concern of the Contractor). The Contractor shall immediately report to the Government all actual or suspected violations of Government

information, personnel, or physical security requirements. The Contractor shall fully comply with all of the reporting requirements that are expressed for specified circumstances and issues identified in discrete Federal Acquisition Regulation or Homeland Security Acquisition Regulation terms in force under this contract.

4. Emergency Situations While on Government Premises. Contractor employees shall immediately report any emergency situations they may witness (any circumstance where actual or potential loss of life, serious injury, or critical damage to property, or other serious incidents, such as fires, or workplace violence, terrorist activities, or other criminal behavior is occurring) per standing TSA procedures while they are performing under contract in government facilities.

5. Government Employee Misconduct. In the event of misconduct by a government employee which is observed or witnessed by a Contractor employee, (or in the event of any unauthorized conduct to which a Government employee may subject a Contractor employee) the Contractor employee shall immediately report such to their on-site Contractor supervisor or other company-designated management official, the Contracting Officer and/or Contracting Officer's Representative.

6. Workplace safety. In the event of any situation involving workplace safety, the Contractor employee shall immediately report such to their on-site Contractor supervisor or other company-designated management official, the Contracting Officer and/or Contracting Officer's Representative.

7. The Contracting Officer may require dismissal from work under this contract and/or removal of access to government facilities, property, information and/or information systems those employees whose conduct the Contracting Officer deems contrary to the public interest or inconsistent with the best interest of national security.

8. Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive but Unclassified, Government procurement sensitive information, and/or other sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

B. **BASIC REQUIREMENTS AFFECTING CONTRACTOR PERFORMANCE**

1. Contractor Responsibility for Performance Management. The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.

2. Limitation on Government Liability. The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.

3. Responsibility for Effective Contract Transitions. A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition. See below Section K -- INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS.

4. The Government observes the following holidays (and government facilities are generally closed on these days, or restricted access or entrance requirements may apply due to security procedures):

New Year's Day
Martin Luther King, Jr. Birthday
Washington's Birthday (President's Day)
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

a) In addition to the days designated as holidays, the Government observes also the following days:

- Any other day designated by Federal Statute, and
- Any other day designated by Executive Order, and
- Any other day designated by President's Proclamation, such as extreme weather conditions.
- Inauguration Day (Washington, DC metropolitan area) (Likewise government facilities in the DC area are generally closed on these days, or restricted access or entrance requirements may apply due to security procedures):

b) When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Representative. Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract.

c) In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursement and time

and materials (T&M)/ labor hour (LH) contracts, the Government will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

Otherwise, the management responsibility for contractor functions approved by the Contracting Officer for offsite work, in the event of inaccessibility of federal workplaces, is the sole responsibility of the contractor. The contractor may propose telework or other solutions when critical work is required, however, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location, and all resources necessary to complete such performance.

d) In the event of an actual emergency, the Contracting Officer may direct the contractor to change work hours or locations or institute telework, utilize personal protective equipment, or other mandated items.

e) In the event of a Government closure (furlough) caused by a lapse in appropriations, which can occur at the beginning of a fiscal year if no funds have been appropriated for that year, or upon expiration of a continuing resolution if a new continuing resolution or appropriations law is not passed, the Contractor shall continue performance under the contract unless otherwise instructed in writing by a Contracting Officer. Unless the Contractor is provided a formal notification to the contrary, usually via a Stop Work Order pursuant to FAR 52.242-15, the Contractor must continue to comply with all terms and conditions of the contract. If a contract will not be affected by a shutdown, generally no separate notification or communication of that fact will be provided. Processing of contractor invoices for payment may or may not be deemed an excepted duty during a furlough. As such, contractor performance is expected even though invoices are pending payment processing. The Prompt Payment Act still applies.

(f)1) Department of Homeland Security (DHS) may close a DHS facility for all or a portion of a business day as a result of-

(A) Granting administrative leave to non-essential DHS employees (e.g., unanticipated holiday);

(B) Inclement weather;

(C) Failure of Congress to appropriate operational funds;

(D) Or any other reason.

(2) In such cases, contractor personnel not classified as essential, i.e., not performing critical round-the-clock services or tasks, who are not already on duty at the facility shall not report to the facility. Such contractor personnel already present shall be dismissed and shall leave the

facility. The contractor is responsible for notifying all of its affected personnel in such circumstances once the Contracting Officer or Contracting Officer's Representative provides notice of such.
(3) The contractor agrees to continue to provide sufficient personnel to perform continual requirements of critical tasks already in operation or scheduled for performance during the period in which DHS employees are dismissed, and shall be guided by any specific instructions of the Contracting Officer or his/her duly authorized representative.

(g) When contractor personnel services are not required or provided due to closure of a DHS facility as described in this term, the contractor's payment under the contract shall be affected as follows--

(1) For cost-reimbursement, time-and-materials and labor-hour type contracts, DHS shall not reimburse as direct costs, the costs of salaries or wages of contractor personnel for the period during which such personnel are dismissed from, or do not have access to, the facility.

(2) For fixed-price contracts, the price will not be prorated and the contractor is expected to satisfy the contract requirement during the period of performance without requested extension.

3) The Government may also terminate a contract for convenience either in partial or full.

C. **CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES**. If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

D. **CONTRACTOR EMPLOYEE TRAINING REQUIREMENTS**. The contractor shall provide fully trained and experienced personnel. Training of contractor personnel shall be performed by the contractor at its expense, except as directed by the Government through written authorization by the Contracting Officer to meet special requirements peculiar to the contract. The Contracting Officer's Representative will identify any specified government training which the contractor's employees with access to TSA IT accounts will be required to complete as a precursor to or coincident with their authorized access to or use of government space or facilities, equipment, information, or information systems as a necessary component of performance required under the contract. Contractor employees are responsible for providing required evidence of timely training completion when the Government assigns such training. Training includes attendance at seminars, symposia or user group conferences. Training will not be authorized for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer

languages and computer operating systems that are available on the commercial market or required by a contract. This includes training to obtain or increase proficiency in word processing, spreadsheets, presentations, and electronic mail.

E. **COOPERATION WITH AUDITORS AND INVESTIGATORS**. The Contractor shall cooperate fully with all auditors and investigators on all matters arising under or directly related to this contract and/or any other matter that may occur in relation to the contractor's presence within Government facilities or due to access to Government information, information systems, property or equipment.

F. **EMPLOYEE REMOVAL**. The Government may identify to the Contractor any contractor employee for removal from contract performance upon notification of failure to comply with the requirements herein.

G. **EMPLOYEE TERMINATION**. The contractor shall notify the Contracting Officer and the Contracting Officer's Representative within 48 hours when an employee performing work under this contract who has been granted access to government information, information systems, property, or government facilities access terminates employment, no longer is assigned to the contract, or no longer requires such access. The contractor shall be responsible for returning, or ensuring that employees return, all DHS/TSA -issued contractor/employee identification, all other TSA or DHS property, and any security access cards to Government offices issued by a landlord of commercial space.

H. **PERSONNEL CHANGES**. The Contractor shall notify the Contracting Officer's Representative (COR) in writing of any changes needed in building, information systems, or other information access requirements for its employees in order to meet contract requirements not later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to the COR: full name, social security number, effective date, and reason for change.

I. **SUBSTITUTION OF KEY PERSONNEL .** The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract's requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

1. an explanation of the circumstances necessitating the substitution;
2. a complete resume of the proposed substitute; and
3. any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

J. **FAILURE TO COMPLY**. Any failure by the Contractor to comply with these requirements may result in a contract termination and/or any other remedy available to the Government, up to and including criminal prosecution where provided for by law.

K. INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS. The TSA may enter into contractual agreements with other Contractors (i.e., "Associate Contractors") in order to fulfill requirements separate from the work to be performed under this contract, yet having a relationship to performance under this contract. It is expected that contractors working under TSA contracts will have to work together under certain conditions in order to achieve a common solution for TSA. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant Contracting Officer (CO) and/or designated representative in providing suitable, non-conflicting technical and/or management interface and in avoidance of duplication of effort. Information on deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.

Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant CO and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.

Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a "lead Contractor" for the project. In these cases, the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.

L. **PERSONAL SERVICES.**

"Personal services" are those in which contractor personnel would appear to be, in effect, Government employees via the direct supervision and oversight by Government employees. No personal services shall be performed under this contract. No Contractor employee will be

directly supervised by a Government employee. All individual Contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor of the Contractor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

The Contractor shall not perform any inherently Governmental actions as defined by FAR 7.500. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change any contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.

The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this term. Nothing in this special contract requirement shall limit the Government's rights in any way under any other term of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this special contract requirement shall be included in all subcontracts at any tier.

Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

(End of term)

L. 5200.233.001 AVAILABILITY OF INTERNAL APPEAL PROCESS PER FAR 33.103 (JUL 2018)

In the event of receipt of the Contracting Officer's final decision of an agency-level protest in accordance with Federal Acquisition Regulation 33.103, the offeror is hereby advised that an appeal process is available from within the agency. The Assistant Administrator of the Contracting and Procurement in the Transportation Security Administration is the independent appeal authority. All appeals must be submitted in writing and signed by a company official who is authorized to commit the company and contain the same elements required in FAR 33.103(d) as well as an explanation of the Contracting Officer's decision (and copy of such decision). Appeals must be sent either in writing or via email to Transportation Security Administration, ATTN: APPEAL OF AGENCY PROTEST, Contracting and Procurement, 601

S. 12th Street, Arlington, VA 20598-6025 , or via email to TSAProcurementPolicy@tsa.dhs.gov. The subject line for the email should clearly indicate "APPEAL OF AGENCY PROTEST".

(End of term)

SECTION 4 – FAR CLAUSES and PROVISIONS

Clauses and provisions from the Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) are incorporated in this document and by reference and in full text. Those incorporated by reference have the same force and effect as if they were given in full text.

CLAUSE	TITLE	DATE
52.204-7	System for Award Management	OCT 2018
52.204-16	Commercial and Government Entity Code Reporting	JUL 2016
52.204-18	Commercial and Government Entity Code Maintenance	JUL 2016
52.204-19	Incorporation by Reference of Representations and Certifications.	DEC 2014
52.212-1	Instructions to Offerors - Commercial Items.	OCT 2018
52.212-4	Contract Terms and Conditions--Commercial Items.	OCT 2018
52.212-5	Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items.	AUG 2019

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items.

CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(a) Provisions.

No provisions are applicable.

(b) Clauses.

3052.204-71 Contractor Employee Access.

3052.215-70 Key Personnel or Facilities.

3052.228-70 Insurance.

3052.236-70 Special Provisions for Work at Operating Airports.

3052.247-72 F.o.B. Destination Only.

(End of clause)

SECTION 5 - QUOTE SUBMISSION AND EVALUATION FOR AWARD

Quotes are due via electronic mail no later than 4:00 PM local time, on Friday August 30, 2019 to patricia.klimowicz@tsa.dhs.gov with copy to susan.messina@tsa.dhs.gov. Questions regarding this RFQ are due no later than 4:00 PM local time, on Monday, August 26, 2019 to patricia.klimowicz@tsadhs.gov with copy to susan.messina@tsa.dhs.gov.

Award will be conducted and evaluated under the Simplified Acquisition Procedures and made on a lowest price technically acceptable (LPTA) basis. Technical tradeoffs will not be made and no additional credit will be given for exceeding acceptability. Award will be made to the Quoter offering the lowest priced, technically acceptable offer that is also determined responsive and responsible (in accordance with FAR 9.1).

The Quoter must limit its quote to no more than 2 pages which does not include any Offeror's "fill-ins" to the RFQ, e.g. schedule of supplies/services, TSA Clauses.

In addition to submitting pricing in Section 1, the Quoter must state 1) that they agree to meet all requirements of the Statement of Work (SOW) and 2) that they possess relevant corporate experience providing the same services required under the SOW. A minimum of three (3) past performance references must be provided as follows:

Description of Services Provided and how they are similar to the services required under this RFQ:	
Customer (Agency or Company):	
Period of Performance:	
Total Estimated Value:	
Reference Point of Contact (Name, Title, email address, and phone number):	

To determine if a quote is technically acceptable, the Quoter must demonstrate that they will meet all technical requirements and have a history of delivering services successfully in the areas described in the RFQ to various organizations. Failure to meet any of the requirements described in this RFQ shall deem the entire quotation as technically unacceptable. Note that TSA reserves the right to use other relevant past performance information it obtains through other sources including other agency databases and information contained in trade literature in its evaluation.